Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Tracking the Stealthy Movements of Vidar Info-Stealer Malware

Date of Publication	Admiralty Code	TA Number
January 23, 2023	A1	TA2023039

Summary

First appeared: 2018
Attack Region: Worldwide
Attack: Vidar is a sophisticated info-stealer malware known for its ability to steal various types of information and its operators are taking steps to evade detection by using Russian VPN gateways, migrating to Tor network and expanding their infrastructure.

Attack Regions

Attack Details

#1

Vidar is an info-stealer malware that was first spotted in the wild in late 2018. It is considered a distinct fork of the Arkei malware family and has a simple business model where customers pay between $130 and $750 for a subscription, with the option to customize the targeted information types. The malware is designed to steal various types of information including browser histories, cookies, credentials, cryptocurrency wallets, and two-factor authentication software data. The delivery methodology for Vidar has varied over time, utilizing email/phishing lures and 'poisoned' cracked software targeting vendors such as AnyDesk and Windows.

#2

A recent analysis of Vidar's infrastructure revealed that Russian VPN gateways are potentially providing anonymity for Vidar operators/customers, making it more challenging for analysts to have a complete overview of this threat. Additionally, the operators appear to be expanding their infrastructure, and have split it into two parts; one for regular customers and the other for the management team and potentially premium/important users. The main website has also been moved to a new domain, my-odin[.]com and the SSL certificate was updated, likely to erase the trail to the new site. It is expected that there will be an increase in campaigns in the upcoming weeks.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
T1047 Windows Management Instrumentation	T1129 Shared Modules	T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading
T1070 Indicator Removal	T1070.004 File Deletion	T1497 Virtualization/Sandbox Evasion	T1497.001 System Checks
T1027 Obfuscated Files or Information	T1005 Data from Local System	T1003 OS Credential Dumping	T1056 Input Capture
T1552 Unsecured Credentials	T1552.002 Credentials in Registry	T1518.001 Security Software Discovery	T1018 Remote System Discovery
T1057 Process Discovery	T1082 System Information Discovery	T1083 File and Directory Discovery	T1518 Software Discovery
T1071 Application Layer Protocol	T1095 Non-Application Layer Protocol	T1105 Ingress Tool Transfer	T1573 Encrypted Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	13e384c54054a094b8045928c8ec9d3697372e551e4887b4ea9e18e319f0f40b 89710436ac93f0216ddd9338d76d1dcbf3cfb3991d72ae1a1d310eeb3699c439
URLs	https[:]//t[.]me/tgdatapacks https[:]//t[.]me/year2023start https[:]//t[.]me/jetbim https[:]//steamcommunity[.]com/profiles/76561199469677637 https[:]//steamcommunity[.]com/profiles/76561199467421923 https[:]//steamcommunity[.]com/profiles/76561199471266194

TYPE	VALUE
Domains	my-odin[.]com bofbot[.]com new.my-odin[.]com old.my-vidar[.]com spaceris[.]com uaery[.]top
IPv4	186[.]2[.]166[.]15 186[.]2[.]166[.]10 94[.]231[.]205[.]192 194[.]99[.]22[.]147 185[.]173[.]93[.]98 5[.]252[.]176[.]64 185[.]243[.]215[.]136 175[.]120[.]254[.]9 187[.]232[.]159[.]164

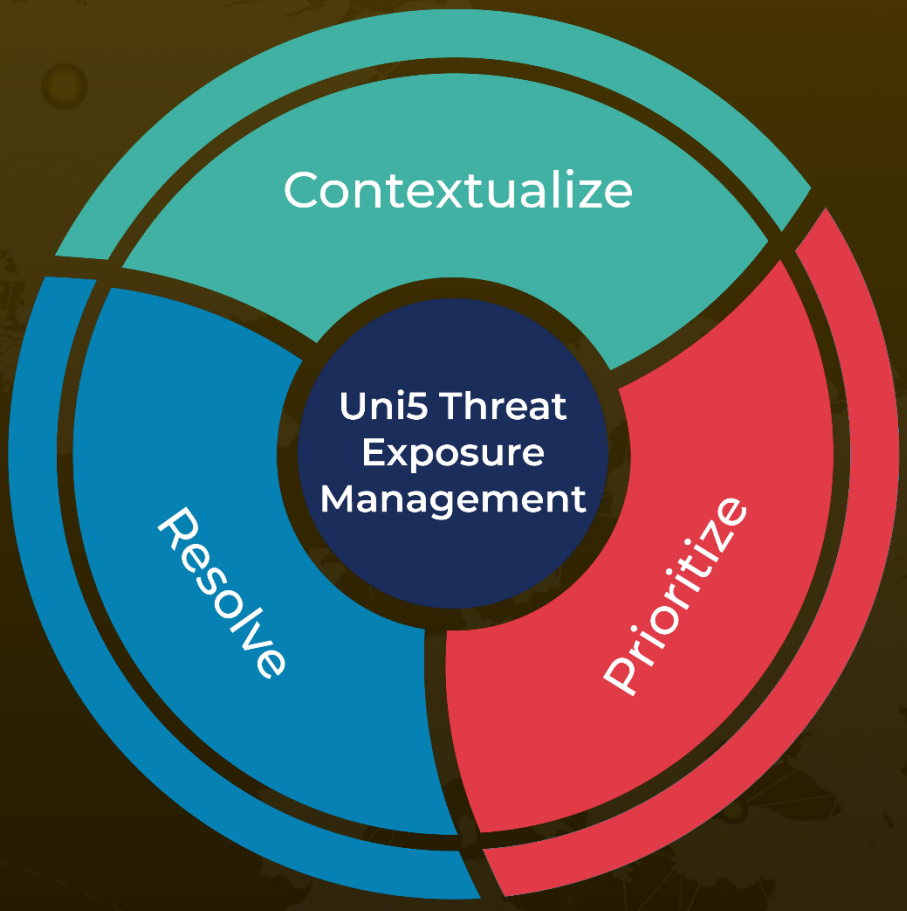
References

https://www.team-cymru.com/post/darth-vidar-the-dark-side-of-evolving-threat-infrastructure

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 23, 2023 • 3:30 AM

More at www.hivepro.com